920537-905630

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

| | |
|---|---|
| IN RE THE APPLICATION OF | ) |
| | ) Examiner: Brandon S. Hoffman |
| Clive Jones | ) |
| | ) |
| SERIAL NO.: 09/913,785 | ) Group Art Unit: 2136 |
| | ) |
| FILED: January 4, 2001 | ) Customer Number: 23644 |
| | ) |
| FOR: Data Encoding/Decoding Device and Apparatus Using the Same | ) |
| | ) |

**BRIEF ON APPEAL**

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

This brief is being filed in view of the Notice of Appeal lodged with the Patent and Trademark Office on December 1, 2006. The Examiner's final Office Action is dated September 1, 2006.

It is believed that no brief fee is due pursuant to 37 C.F.R. §41.20(b)(2), since with the Appeal mailed December 23, 2005 and received by the Patent and Trademark Office on December 27, 2005, the brief fee of $500.00 was paid, but the Examiner subsequently withdrew the application from the Appeal, and issued a further Office Action which ultimately lead to reinstatement of the Appeal. Should any fee be due, however, that fee may be deducted from Deposit Account No. 12-0913 after telephone authorization by the undersigned.

**(i) Real Party in Interest**

This application is assigned to Meridian Audio Ltd., who is the real party in interest. The assignment was recorded on January 14, 2002 at reel 0124777, frame 0546.

**(ii) Related Appeals and Interferences**

There are no known related appeals and interferences

**(iii) Status of Claims**

This application was filed with claims 1 through 18, and in a response mailed March 24, 2005, claims 11-18 were cancelled, and claims 19 through 22 were added. By an amendment filed to support the earlier Notice of Appeal received by the Patent and Trademark office on October 31, 2005, claims 1-7 and 19-20 were cancelled. In reopened prosecution following the earlier appeal, no claim amendments were made, and those claims being appealed are claims 8-10, 21 and 22. The claims are set forth in the Claims Appendix appended hereto.

**(iv) Status of Amendments**

No claim amendments or response have been filed following the September 1, 2006 final Office Action.

**(v) Summary of Claimed Subject Matter**

A problem occurs when transmitting audio data digitally for output. The problem is that sound is output in the analog domain which means that the final drivers driving loudspeakers, headphones etc must inevitably operate in the analog domain, and such drivers are sensitive to picking up the digital signal. A digital signal normally has sharp peaks at certain frequencies, often frequencies related to the clock frequency, and so the digital signal picked up in analog stages can produce a significant degradation in the output quality.

A further factor in the choice of digital signal is the need to be able to recover the clock signal from the transmitted digital signal at the receiving end.

Finally, encoding is often needed when transmitting data, for example to ensure that the digital signals cannot be captured by any device, for example to protect digital audio signals from illegal recording. This gives rise to a further difficulty, in that it is necessary to transmit the encoding key from the transmitter to receiver and this occupies bandwidth in the channel. It is therefore desired to minimize the number of transmitted bits, while still encoding securely.

Thus, what is needed is a way of encoding digital audio data to deal with all these issues.

Claim 8

The invention solves this problem with the apparatus of claim 8. Each bit input into the data encoding device 20 (Figs. 3, 4) is encoded separately to create an encoded output bit 28, and the encryption key is updated after encoding each bit of a word (page 8, line 12 - page 9, line 20).

The design enables the encoded output data to have the properties of white noise so reducing possible interference in analog stages as well as improving the performance of clock recovery in the decoder, while at the same time maintaining the data structure so that standard interface protocols can be used (page 9, lines 23 to 29).

The design also maintains security even if only a limited number of random bits are transmitted from encoder to decoder, for example when transmitting only one new random bit for each word. However, this means that there is a link between the random numbers used to encode subsequent words. In the invention, this relationship is disguised by not simply applying the bits generated by the random number generator, but by using a further unit, the permutation unit, which generates an initial plurality of encoding bits, which as stated in the claim is the encryption key used to generate the initial output bit. Thus, the permutation unit makes it much harder for an eavesdropper to correctly decode the transmitted signal (page 10, line 23 - page 13, line 13).

Claims 21 and 22

The above discussion also applies to claims 21 and 22.

**(vi) Grounds of Rejection To Be Reviewed On Appeal**

There is one ground of rejection being reviewed on appeal, the rejection of claim 8-10, 21 and 22 under 35 U.S.C. §103(a) as being unpatentable over Baker (U.S. 5,946,355) in view of Bright et al (U.S. 4,893,339).

**(vii) Argument**

Claims 8 stand rejected over Baker in view of Bright et al. The Examiner contends that Baker discloses an encoding unit which combines each bit input on the serial data input with a plurality of additional encoding bits forming an encryption key to derive an encoded output bit.

In making the above assertion, the Examiner argues that the Linear Feedback Shift Register (LFSR) in Baker (Figure 2, reference number 12) represents, at any given time, the current encryption key.

In fact, as stated at Column 1, lines 22-27 of Baker, the LFSR is a scrambler that is used to eliminate longs strings of "1"s and "0"s in serial data (see also Column 1, lines 39-40 of Baker). As is well known to the skilled person in the art, LFSR's are used to generate a pseudo-ransom sequence. However, since the output streams of a LFSR are linear and deterministic, use of a LFSR is limited to "randomizing" a bit stream. Those skilled in the art will know that LFSRs are not to be used for encryption or encipherment, because scrambling with LFSRs does not protect the information from eavesdropping. Thus, Baker describes a "keyless" scrambling system wherein the output only depends on the input.

Accordingly, the LFSR of Baker is not an encoding unit which is used to form an encryption key to derive an encoded bit, and the skilled reader would not interpret Baker as teaching the LFSR to be an encoding unit. Baker, instead, describes the coding unit of the transmitter to be the Non-Return to Zero Inverted (NRZI) coder (Figure 2, reference

numeral 14). In the first whole paragraph of column 2, Baker details the NRZI coder as being a single-bit LSFR which acts as a modulo-two accumulator to change the output where a logic "1" is input and to cause no change in the output when a logic "0". This simple coding process can then be easily decoded as explained at Column 2, lines 17-20, of Baker.

For the above reasons, it is submitted that Baker does not disclose an encoding unit as recited in pending claim 8. However, for completeness we also submit the following comments, in the event that the LFSR of Baker is taken to be an encoder contrary to normal practice in the art.

From Figure 2 of Baker, it can be seen that the LFSR combines each bit input on the serial data input with a single additional bit, not a plurality of additional encoding bits as specifically recited by pending claim 8. The Examiner contends that the single bit inputted from the serial data input is combined with a plurality of additional coding bits which make up the encryption key.

The Examiner's assertion is refuted for the reason that the LFSR simply combines each serial input data bit with a single additional bit. The LSFR of Baker does not combine each input bit with a plurality of additional (encoding) bits forming as recited in pending claim 8. From the present application as filed it will be understood the plurality of additional bits form an encryption key, i.e. the encryption key comprises a plurality of encoding bits and not just a single bit (see page 9, lines 18-20, of the specification, and pending claim 8).

The Examiner acknowledges that Baker does not teach the features of the random generator and the transformation unit as recited in pending claim 8. However, for the above mentioned reasons, it is further asserted that Baker does not disclose the feature of "an encoding unit which combines each bit on the serial data input with a plurality of additional bits forming an encryption key".

The Examiner is also of the mistaken opinion that Bright et al teaches the additional features not present in Baker.

Bright et al describes and encryption system using a random number. However, in Bright et al, only the random number is used to produce the encryption key. Thus, the incoming data is not used to generate the encryption key in the system of Bright. In other words, the updated keys do not depend on the input data.

It is therefore submitted that combination of the teachings of Baker and Bright et al does not produce a data encoding device as recited in pending claim 8. More specifically, they do not disclose or suggest forming an encryption key comprising a plurality of bits which is derived from previous values of the encryption key and the input bit.

With regard to independent claim 21, the above detailed reasoning is also applies in respect of the decoding apparatus disclosed by Baker and Bright et al. More specifically, it is again noted that Baker does not teach the features of a transformation unit and a decoding unit as recited in pending claim 21. Also, no combination of Baker and Bright et al will produce a data decoding device in which the serial data input is decoded with a key comprising a plurality of bits which is derived from previous values of the key and of the input bit.

Finally, in accordance with the above, it is respectfully submitted that pending independent claim 22 is not taught by any combination of the cited prior art references, since claim 21 is directed to a data communications system comprising an encoding device of claim 8 and a decoding device of claim 21.

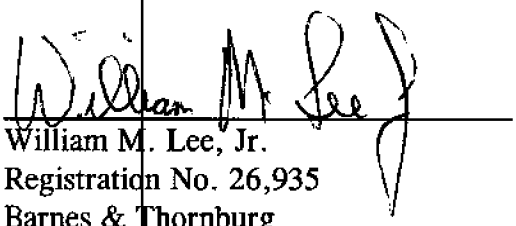
For the avoidance of any doubt, the reasoning and arguments that were previously submitted to support the previous responses filed for this application are hereby maintained.

**Conclusion**

For the reasons set forth above, it is submitted that the Examiner's rejection of claims 8-10, 21 and 22 has been demonstrated to be in error, and reversal of the Examiner's rejections is therefore requested.

December 21, 2006

Respectfully submitted,



William M. Lee, Jr.
Registration No. 26,935
Barnes & Thornburg
P.O. Box 2786
Chicago, Illinois 60690-2786
(312) 214-4800
(312) 759-5646 (fax)

## Claims Appendix

1 - 7. (cancelled)

8. An apparatus for generating digital audio data comprising

a source of digital audio signals, and

a data encoding device having:

a serial data input;

an encoded serial data output;

a random number generator which generates a stream of random bits;

a transformation unit comprising means for storing a predetermined number of values of the random bit to derive a multiple bit random word;

a permutation unit which generates an initial plurality of encoding bits from the multiple bit random word; and

an encoding unit which combines each bit input on the serial data input with a plurality of additional encoding bits forming an encryption key, to derive an encoded output bit and an updated encryption key comprising a plurality of updated encodes bits, wherein an initial bit input on the serial data input is encoded with an encryption key comprising the initial plurality of encoding bits output by the permutation unit and each subsequent input bit is encrypted using an updated key which is derived from previous values of the encryption key and of the input bit, and wherein over time the encoded output bit stream comprises substantially white noise.

9. An apparatus as claimed in claim 8, wherein the output at the output port is in SPDIF or AES/EBU format.

10. An apparatus as claimed in claim 8, comprising a compact disc player.

11 - 20. (cancelled)

21. An apparatus for reconstructing digital audio signals comprising:

an input for receiving encoded digital audio signals;

a receiver for supplying the encoded digital audio signals to a decoding device;
and an output for the reconstructed digital audio signal; and
a decoding device comprising:
a serial data input;
a transformation unit comprising means for storing a predetermined number of values of random bits to derive a multiple bit random word;
a permutation unit which generates an initial plurality of bits from the multiple bit random word; and
an decoding unit which combines each bit input on the serial data input with a plurality of additional encoding bits forming a key, to derive an decoded output bit and an updated key comprising a plurality of updated bits, wherein an initial bit input on the serial data input is decoded with a key comprising the initial plurality of bits output by the permutation unit and each subsequent input bit is decrypted using an updated key which is derived from previous values of the key and of the input bit.

22. A data communications system comprising:
a data encoding device comprising:
a serial data input;
an encoded serial data output;
a random number generator which generates a stream of random bits;
a transformation unit comprising means for storing a predetermined number of values of the random bit to derive a multiple bit random word;
a permutation unit which generates an initial plurality of encoding bits from the multiple bit random word; and
an encoding unit which combines each bit input on the serial data input with a plurality of additional encoding bits forming an encryption key, to derive an encoded output bit and an updated encryption key comprising a plurality of updated encodes bits, wherein an initial bit input on the serial data input is encoded with an encryption key comprising the initial plurality of encoding bits output by the permutation unit and each subsequent input bit is encrypted using an updated key which is derived from previous values of the key and of the input bit, and wherein over time the encoded output bit stream comprises substantially white noise; and

a decoding device comprising:

a serial data input;

a transformation unit comprising means for storing a predetermined number of values of random bits to derive a multiple bit random word;

a permutation unit which generates an initial plurality of bits from the multiple bit random word; and

an decoding unit which combines each bit input on the serial data input with a plurality of additional encoding bits forming a key, to derive an decoded output bit and an updated key comprising a plurality of updated bits, wherein an initial bit input on the serial data input is decoded with a key comprising the initial plurality of bits output by the permutation unit and each subsequent input bit is decrypted using an updated key which is derived from previous values of the key and of the input bit.

## Evidence Appendix

None.

## Related Proceedings Appendix

None.